IN THE CLAIMS

Please amend the claims as follows:

Claims 1-10 (Canceled).

Claim 11 (New): A method of transmitting service data between a first telecommunication device and a second telecommunication device of a telecommunication network, a central module generating prepaid access data, the prepaid access data comprising a first digital key and control data, and the prepaid access data being stored in a memory module of the first telecommunication device, and the central module generating a second digital key, assigned to the first digital key, the second digital key being stored on one or more control units of the telecommunication network, wherein

the first telecommunication device determines a validity criterion based on control data of the prepaid access data, and encodes service data of the first telecommunication device by the first key, as long as the validity criterion is fulfilled, and

the first telecommunication device transmits encoded service data to the control unit, the control unit checking by the second digital key that the encoded service data are encoded with the first digital key, upon a successful check the control unit decoding the encoded service data, and the control unit transmitting the decoded service data to the second telecommunication device.

Claim 12 (New): The method according to claim 11, wherein the prepaid access data stored in the memory module of the first telecommunication device are modified and/or deleted during the encoding of service data.

Claim 13 (New): The method according to claims 11, wherein the prepaid access data stored in the memory module of the first telecommunication device include a monetary amount value, the monetary amount value being modified and/or deleted during the encoding of service data.

Claim 14 (New): The method according to claim 11, wherein the prepaid access data are stored on an SIM module of the first telecommunication device.

Claim 15 (New): The method according to claim 11, wherein the encoding of the service data includes a digital encryption and/or digital signature, and the decoding of the service data includes a corresponding digital decryption and/or verification of a digital signature.

Claim 16 (New): The method according to claim 11, wherein the prepaid access data include an authorization for the encoding of a definable quantity of service data, the prepaid access data being deleted as soon as the encoding of the definable amount of service data has been completed.

Claim 17 (New): The method according to claim 11, wherein a multiplicity of blocks with prepaid access data are storable in the memory module of the first telecommunication device.

Claim 18 (New): The method according to claim 11, wherein the control data comprise a multiplicity of blocks, the determination of a validity criterion as well as the

modification or deletion of the corresponding block of control data being feasible for each block.

Claim 19 (New): A system for carrying out the method according to claim 11, with a first telecommunication device, including an SIM module, with a MSC (Mobile Switching Center) connectible to the first telecommunication device via a telecommunication network, a central module comprising means for generation of prepaid access data with a first digital key and with control data and a corresponding second digital key, the SIM module of the first telecommunication device comprising means for storing the prepaid access data, and the MSC comprising means for storing the second digital key, wherein

the first communication device comprises means for checking the validity criteria of prepaid access data stored in the memory module, for encoding service data of the first communication device by the first digital key and for transmitting the encoded service data to the MSC, and

the MSC comprises means for checking the encoded service data by the second digital key, for decoding the encoded service data and for transmitting the service data to a second telecommunications terminal.

Claim 20 (New): The system according to claim 19, wherein the first telecommunication device includes an encryption module or a signature module for encryption or signature of service data by the first digital key, and the MSC comprises a decryption module or a signature verification module for decryption or verification of the signature of encrypted or signed service data by the second digital key.